Dansk persondataret

Bent Ole Gram Mortensen (red.)

Dansk persondataret

Ex Tuto
PUBLISHING
www.extuto.com

Bent Ole Gram Mortensen (red.), Carina Risvig Hamer, Daniel Hartfield-Traun, Lisa Hjerrild, Kent Kristensen, Jesper Kruse Markvart, Helene Arensbak Mørk, Jesper Løffler Nielsen, Ayo Næsborg-Andersen, Sten Schaumburg-Müller, Christian Højer Schjøler, Peter Starup, Jøren Ullits & Frederik Waage
Dansk persondataret
Første udgave, første oplag

Denne bog er udgivet i januar 2020 af Ex Tuto Publishing A/S. Grafisk tilrettelæggelse og sats af mere.info A/S, som har anvendt LibreOffice/Linux samt skrifterne Baskerville Original og Cronos designet af henholdsvis František Štorm i 2000 og Robert Slimbach i 1996. Jan Trzaskowski har stået for forlagsredaktion og Tove Møgelvang-Hansen har været ansvarlig for korrekturlæsning. Bogen er trykt på Munken Pure 100 g/m^2 af Narayana Press, der ligger på Gyllingnæs syd for Odder. Indbindingen er udført af Buchbinderei S.R. Büge GmbH i Celle. Bogen er fagfællebedømt.

Ex Tuto A/S er medlem af Forening for Boghaandværk, og vi støtter bæredygtig skovforvaltning ved at anvende FSC-certificeret papir.

Printed in Denmark 2020
ISBN 978-87-420-0033-5

Ex Tuto Publishing A/S
Toldbodgade 55, 1.
DK-1253 København K
www.extuto.com

MIX
Papir fra ansvarlige kilder
FSC® C010651
www.fsc.org

Udgivet med støtte fra
dreyersfond

FairPublishing

Kapiteloversigt

Kapitel 10

Ansvarssubjekter og aftaleregulering

Jesper Løffler Nielsen & Helene Arensbak Mørk

10.1. Introduktion

Persondataforordningen har til formål at sikre, at de der behandler personoplysninger, gør dette korrekt og lovligt, dvs. i overensstemmelse med forordningens krav. Det er derfor relevant at se på, hvem det egentlig er, der bliver pålagt forpligtelser i forordningen. I dette kapitel ses der nærmere på forordningens ansvarssubjekter og de samarbejdskonstruktioner, der kan opstå imellem dem, herunder kravene der stilles i forordningen til reguleringen heraf.

Det er vigtigt at understrege, at placeringen af dataansvar kan virke simpelt i teorien, men ofte volder store problemer i praksis. Nedenfor vil det primære fokus være på den mere generelle og teoretiske gennemgang, suppleret med enkelte praktiske eksempler.

Kapitlet har følgende opbygning: afsnit 10.2. gennemgår de ansvarssubjekter, der er omfattet af forordningens regler. Afsnit 10.3. omhandler selve aftalegrundlaget imellem ansvarssubjekterne, og afsnit 10.4 uddyber den praktiske håndtering af databehandlerkonstruktionen med udgangspunkt i databehandleraftalens livscyklus.

10.2. Ansvarssubjekterne

Overordnet findes der to kategorier af ansvarssubjekter i forordningen: *Dataansvarlige* og *databehandlere*. Hertil kommer underkategorierne *fælles dataansvar* og *underdatabehandlere*.

Rubriceringen af, hvilken type ansvar man falder ind under i en given situation, har en række væsentlige konsekvenser. *For det første* er der stor forskel på, hvilke krav man bliver underlagt. *For det andet* kan rollefordelingen få stor betydning for placering af et eventuelt straffeansvar, idet det er muligt for både den dataansvarlige og databehandleren at ifalde ansvar for overtrædelse af forordningen. *Sidst*, men ikke mindst har ansvarsfordelingen stor betydning for de registrerede, idet rubriceringen er afgørende for, hvem de kan udøve deres rettigheder overfor.

10.2.1. Dataansvarlig

I artikel 4, stk. 7, defineres en dataansvarlig som

> "en fysisk eller juridisk person, offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger [...]"

Ansvaret for behandling af personoplysninger – og derved opfyldelsen af kravene hertil efter forordningen – ligger som udgangspunkt hos den dataansvarlige. Her kan f.eks. nævnes det helt overordnede ansvar for, at forordningens bestemmelser overholdes, og at dette dokumenteres (artikel 5, stk. 2), ansvaret for opfyldelse af oplysningspligten (artikel 13 og 14) og håndtering af anmodninger fra den registrerede samt kravene til kommunikation med denne (artikel 12), ligesom ansvaret for anmeldelse af og underretning om brud på persondatasikkerheden (artikel 33 og 34) ligger hos den dataansvarlige. Lidt forsimplet kan man sige, at den dataansvarlige skal overholde alle krav i forordningen.

10.2.1.1. Hvem kan være dataansvarlig?

Som det fremgår af definitionen, kan den dataansvarlige være "en fysisk eller juridisk person, offentlig myndighed, en institution eller et

andet organ". Oftest vil der være tale om virksomheder eller offentlige myndigheder.

Det kan ikke udelukkes, at privatpersoner kan være dataansvarlige. Dette vil i høj grad afhænge af behandlingens karakter, herunder om forholdet bliver omfattet af undtagelsen i artikel 2, stk. 2, litra c.[1]

En forening vil også kunne være dataansvarlig for foreningens behandling af personoplysninger, hvis foreningen har beslutningskompetencen til behandlingen.[2]

10.2.1.2. Den der afgør formål og hjælpemidler

Det afgørende ved vurderingen af, hvem der agerer dataansvarlig, er, om den pågældende har kontrollen over (afgør) formålet med behandlingen, og med hvilke hjælpemidler der må foretages behandling.

Det er altså den dataansvarlige, der bestemmer, *hvorfor* personoplysninger skal behandles, samt tager de væsentligste behandlingsskridt, herunder indsamling, sletning og videregivelse.[3]

For så vidt angår *hvordan* oplysningerne behandles, er det værd at bemærke, at dataansvarlige i stigende grad benytter en databehandler til også at fastsætte hjælpemidlerne, da det netop kan være databehandleren, der har kompetencen hertil. Kriteriet om hjælpemidler er derfor ikke af afgørende betydning, men kan være mere flydende, modsat kriteriet om formålet, der alene kan fastsættes af den dataansvarlige.[4]

Vælger en virksomhed f.eks. at hyre en advokat til at hjælpe med en retssag, som virksomheden er en del af, kan advokaten have brug for at behandle personoplysninger om virksomhedens parter. Selvom virksomheden har angivet nøje instrukser til advokaten om behandling af sagen, vil advokaten fortsat have mulighed for at træffe de væsentligste beslutninger om, med hvilke formål og hjælpemidler sagen skal behandles (f.eks. hvilke oplysninger, der skal bruges i retssagen, hvem der skal indkaldes som vidner, og hvor længe oplysningerne skal opbeva-

1. Behandling af personoplysninger, der foretages som led i rent personlige eller familiemæssige aktiviteter (privatreglen), behandles i kapitel 4, afsnit 4.3.
2. Se mere om foreninger i Justitsministeriet 2018.
3. Datatilsynet 2017, s. 9.
4. Løffler Nielsen & Larsen 2019, pkt. 3.2.3.

res). Advokaten vil derfor være selvstændig dataansvarlig for denne behandling af virksomhedens personoplysninger.

10.2.1.3. Fælles dataansvar

Som det fremgår af definitionen af den dataansvarlige i artikel 4, kan der være situationer, hvor flere aktører fastsætter, hvorfor og hvordan der skal ske behandling af personoplysninger. Hvis der er tale om flere dataansvarlige, der sammen afgør formål og til dels hjælpemidler, betegnes konstruktionen *fælles dataansvar*.

Overordnet indebærer fælles dataansvar således, at der er flere parter med til at beslutte, hvorfor og/eller hvordan en given behandling af personoplysninger skal ske.

Et eksempel kunne være, at en gruppe af virksomheder beslutter at tilbyde en samlet rabatordning. Her vil der være fælles dataansvar for den fælles database og behandlinger knyttet til oplysningerne heri, hvorimod hver af de deltagende parter forbliver selvstændigt dataansvarlige for deres egne interne behandlinger.

Før forordningens ikrafttræden var der ganske få eksempler i den juridiske litteratur på fælles dataansvar, herunder i Datatilsynets praksis. EU-Domstolen kom dog i 2018 med nogle afgørelser, som gør det klart, at reglerne om fælles dataansvar fremadrettet vil få en mere fremtrædende rolle. EU-Domstolen har bl.a. slået fast, at fælles dataansvar også kan foreligge, hvor den ene dataansvarlige har en væsentligt større kontrol over eller indflydelse på behandlingen end den anden,[5] samt at den fælles indflydelse på formål og hjælpemidler også kan have en mere uformel karakter.[6]

Med dette potentielt meget brede anvendelsesområde er der en risiko for, at vi er på vej mod et krav om tusindvis, eller snarere millioner, af aftaler om fælles dataansvar. Generaladvokat Bobek rejser netop denne bekymring i sit udkast til afgørelse afsagt 21. december 2018 i *ID Fashion*-sagen, og det bliver derfor interessant at se, om EU-Domstolen

5. EU-domstolens afgørelse af 5. juni 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16", præmis 43.
6. EU-domstolens afgørelse af 10. juli 2018, *Jehovan todistajat* , C-25/17, præmis 67 og 68.

formår at finde en hensigtsmæssig løsning på denne grundlæggende udfordring.[7]

Fælles dataansvar medfører som udgangspunkt, at alle aktørerne er fælles ansvarlige for overholdelsen af de persondataretlige regler, ligesom det er et krav, at det fælles dataansvar reguleres i en aftale, der kommunikeres til omverdenen, se nærmere nedenfor under pkt. 10.3.2. I tilfælde af, at den behandling af personoplysninger, der er omfattet af det fælles dataansvar, udløser et strafansvar, hæfter de dataansvarlige solidarisk, jf. artikel 82, stk. 4. Dette indebærer, at alle parter er fuldt ansvarlige for den samlede forpligtelse. Den enkelte dataansvarlig kan derved blive pålagt at betale det fulde erstatningsbeløb til den, der har lidt skade i forbindelse med den fælles databehandling, og har herefter mulighed for at gøre et krav gældende mod de øvrige aktører, svarende til deres del af ansvaret, jf. artikel 82, stk. 5.

10.2.2. Databehandlere

Databehandleren defineres i artikel 4, nr. 8, som

> "en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne".

Af databehandlerens primære forpligtelser efter forordningen kan nævnes indgåelse af databehandleraftaler (artikel 28), udarbejdelse af fortegnelser over behandlingsaktiviteter, der håndteres på vegne af en dataansvarlig (artikel 30, stk. 2), gennemførelse af passende tekniske og organisatoriske sikkerhedsforanstaltninger (artikel 32) og underretning af den dataansvarlige i tilfælde af brud på persondatasikkerheden (artikel 33, stk. 2).

7. EU-domstolens afgørelse af 29. juli 2019, *Fashion ID*, C-40/17. Sagen omhandler ansvarsfordelingen mellem Facebook og en indehaver af en hjemmeside, som indeholder en "Like"-knap, dvs. et link, som muliggør, at brugeren direkte fra hjemmesiden "Synes godt om" indehaveren af hjemmesidens Facebook-side. Generaladvokaten fastslår under henvisning til sagerne C-210/16 (Facebook) og C-25/17 (Jehovas Vidner), at det er svært at komme udenom et fælles dataansvar (præmis 59-70), men rejser samtidig en bekymring om, hvad en så bred fortolkning af begrebet på sigt kan føre til (præmis 71-93).

Det afgørende for, om aktøren defineres som databehandler, er, hvorvidt den pågældende behandler personoplysninger, og hvorvidt dette sker på den dataansvarliges vegne og efter dennes instruks.

De typiske eksempler på aktører, der behandler personoplysninger på den dataansvarliges vegne og derved agerer databehandlere, er hosting-/cloududbydere, hjemmesideudbydere, systemer til e-mail marketing, løn- og bookingsystemer, udbydere af kommunikationssoftware mv.

10.2.2.1. Underdatabehandlere

Lige såvel som at den dataansvarlige kan gøre brug af databehandlere, kan databehandleren også gøre brug af egne databehandlere. Disse betegnes typisk som *underdatabehandlere* og er reguleret i artikel 28, stk. 2 og 4.

Databehandleren må efter artikel 28, stk. 2, ikke gøre brug af underdatabehandlere uden godkendelse fra den dataansvarlige. En sådan godkendelse kan enten være i form af en *generel* (forudgående) godkendelse til, at databehandleren må bruge underdatabehandlere. I så fald skal databehandleren underrette den dataansvarlige, såfremt der sker ændringer i anvendelsen af underdatabehandlere, og dette skal ske tids nok til, at den dataansvarlige kan nå at gøre indsigelser, inden ændringen iværksættes. En godkendelse kan også bestå af en *specifik* godkendelse, hvorved forstås, at accepten skal indhentes skriftligt forud for hver ændring.

Underdatabehandlere skal i en skriftlig (underdatabehandler-) aftale blive pålagt mindst de samme databeskyttelsesforpligtelser, som den dataansvarlige har pålagt databehandleren. Som led heri forbliver databehandleren ansvarlig over for den dataansvarlige for underdatabehandlerens overholdelse af sine forpligtelser.

10.2.3. Opsamling

Det primære kriterium for afgrænsning af de enkelte roller er altså kontrollen over *formålet*. Det er den *dataansvarlige*, som direkte eller indirekte har besluttet, at de omhandlede personoplysninger skal behandles, og typisk også, hvornår behandlingen skal ophøre. Træffes beslutninger herom af flere dataansvarlige i fællesskab, formelt eller uformelt, vil der være tale om *fælles dataansvar*. Er der derimod tale om, at en

myndighed eller virksomhed er blevet bedt om at behandle personoplysninger på vegne af en anden og alene behandler oplysningerne til dette formål, vil der være tale om en *databehandlerkonstruktion*.

Definitionerne på henholdsvis dataansvarlig, databehandler og fælles dataansvar kan være vanskelige at håndtere i praksis. I nedenstående skema er opstillet supplerende kriterier, som kan anvendes ved fastlæggelsen i praksis:

<table>
<tr>
<td>Dataansvarlig
"[…] afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling […]</td>
<td>Fælles dataansvar
"[…] alene eller sammen med andre afgør […]</td>
<td>Databehandlere"
[…] behandler personoplysninger på den dataansvarliges vegne […]</td>
</tr>
<tr>
<td colspan="2">Følgende beslutninger kan som udgangspunkt alene træffes af en (eller flere) dataansvarlig(e):

— at personoplysninger skal behandles og til hvilke formål, herunder om behandlingen er nødvendig for at opfylde lovkrav
— hvilke personoplysninger der er relevante, nødvendige og lovlige at behandlede
— hvem oplysningerne deles med
— om anmodninger fra registrerede om udøvelse af rettigheder skal imødekommes
— de overordnede rammer for, hvordan oplysningerne skal behandles, herunder det overordnede ansvar for tilstrækkelig sikkerheden
— Hvornår og hvordan oplysningerne slettes og/eller destrueres</td>
<td>En dataansvarlig kan (i databehandleraftalen) overlade følgende beslutninger til en databehandler:

— hvilke it-systemer der skal anvendes til behandlingens
— hvor oplysningerne skal opbevares (digitalt og/eller fysisk)
— konkrete sikkerhedsforanstaltninger
— øvrige vilkår for levering af databehandlerens ydelse, herunder rent kommercielle vilkårene
— valg af underdatabehandlere (dog underlagt den dataansvarliges generelle eller specifikke godkendelse)</td>
</tr>
</table>

10.3. Aftaleregulering af ansvaret

Uanset om der er tale om en databehandlerkonstruktion eller en situation med fælles dataansvar, er der i forordningen krav om, at forholdet reguleres af en aftale imellem aktørerne. Disse gennemgås nedenfor.

10.3.1. Databehandleraftaler

Ifølge artikel 28, stk. 3, skal databehandlerens behandling af personoplysninger på vegne af den dataansvarlige være reguleret af en skriftlig aftale, der er bindende for databehandleren.

Databehandleraftalen og dens indhold uddybes særskilt nedenfor i afsnit 10.4.

10.3.2. Aftaler om fælles dataansvar

Reguleringen af fælles dataansvar findes i persondataforordningens artikel 26. I modsætning til de mere udførlige krav til indholdet af en databehandleraftale i artikel 28 stilles der ikke specifikke krav til indholdet af ordningen mellem de fælles dataansvarlige.

Efter artikel 26, stk. 1, skal de fælles dataansvarlige på en gennemsigtig måde fastlægge deres respektive roller og ansvar for overholdelse af forordningens bestemmelser, navnlig hvad der angår de registreredes rettigheder og oplysningspligten efter artikel 13 og 14. Fastlæggelsen af dataansvaret skal ske ved hjælp af en "ordning" imellem de fælles dataansvarlige, hvis væsentligste dele efter artikel 26, stk. 2, skal gøres tilgængelige for de registrerede. På den måde har de registrerede mulighed for at blive bekendt med, hvilken virksomhed/myndighed, der er ansvarlig for hvad. Dette kan f.eks. opfyldes igennem en privatlivspolitik eller ved offentliggørelse af ordningen.

Den registrerede har – uanset ordningen mellem de fælles dataansvarlige – fortsat mulighed for at udøve sine rettigheder i medfør af forordningen over for den enkelte dataansvarlige, jf. artikel 26, stk. 3.

Datatilsynet har udarbejdet en skabelon vedrørende fælles dataansvar, som kan anvendes direkte eller som inspiration ved udarbejdelse af en aftale. Skabelonen er tilgængelig på Datatilsynets hjemmeside.

10.3.3. Andre samarbejdskonstruktioner

Der er visse tilfælde, hvor en person, virksomhed eller myndighed ikke behandler personoplysninger som en del af aftalen med den dataansvarlige. Her kan det ud fra en konkret vurdering af ydelsens karakter og risiko tale for at pålægge den dataansvarlige en forpligtelse til at foretage visse sikkerhedsmæssige foranstaltninger, f.eks. udarbejdelse af en tavshedspligtserklæring.

Datatilsynet har angivet et eksempel[8] på netop dette:

> "Virksomhed A hyrer en reparatør til at reparere virksomhedens kopimaskine, hvori der kan være gemt dokumenter med personoplysninger. Aftalen mellem virksomhed A og reparatøren går ud på, at reparatøren skal reparere virksomhed A's kopimaskine. Virksomhed A vil i denne situation ikke benytte reparatøren som databehandler, fordi aftalen mellem parterne hverken helt eller delvist går ud på, at reparatøren skal behandle personoplysninger på vegne af virksomhed A. Hvis der er risiko for, at reparatøren i forbindelse med sin reparation får adgang til personoplysninger, kan virksomhed A – som led i sine almindelige sikkerhedsforanstaltninger – bede reparatøren om at underskrive en tavshedspligtserklæring."

10.4. Særligt om databehandleraftaler

I de foregående afsnit er de forskellige typer af ansvarssubjekter og aftalereguleringer blevet uddybet. I dette afsnit ses der nærmere på den aftalekonstruktion, som har størst praktisk relevans; *databehandleraftalen*. I nedenstående skema er oplistet de fem "faser", som en dataansvarlig skal igennem for at sikre, at benyttelsen af databehandlere overholder forordningens krav:

8. Datatilsynet 2017, s. 8.

Fase	Indhold	Uddybning
1	Er der tale om en databehandler?	Se afsnit 10.2.
2	Risikovurdering: Kan den valgte databehandler levere tilstrækkelig sikkerhed i lyset af behandlingens karakter og risici?	Se afsnit 10.4.1.
3	Indgåelse af en databehandleraftale, der lever op til kravene i forordningen.	Se afsnit 10.4.2.
4	Føre systematisk tilsyn med, at databehandleren lever op til forpligtelserne i databehandleraftalen.	Se afsnit 10.4.3.
5	Når databehandleraftalen ophører, skal databehandleren tilbagelevere og/eller slette den dataansvarliges oplysninger.	Se afsnit 8.5.

10.4.1. Den dataansvarliges risikovurdering af databehandleren

Den dataansvarlige er efter artikel 28, stk. 1, forpligtet til udelukkende at anvende databehandlere, der kan garantere tilstrækkelig sikkerhed, og i øvrigt sikre, at behandlingen af personoplysninger kan ske under overholdelse af kravene i forordningen – ikke mindst sikre beskyttelse af den registreredes rettigheder. Alt andet ville da også udvande reglerne, hvis den dataansvarlige kunne slippe for sit ansvar ved blot at bede en anden om at behandle oplysninger på sine vegne.

Det er derfor – især som dataansvarlig – vigtigt at sikre sig, at det af aftalen fremgår, at der skal arbejdes risikobaseret, samt hvilke konkrete tekniske og organisatoriske sikkerhedsforanstaltninger[9] databehandleren som minimum har gennemført til sikring af den dataansvarliges oplysninger.

9. Se herom i kapitel 14.

Af konkrete sikkerhedsforanstaltninger kan eksempelvis nævnes fysisk adgangsbegrænsning, backup og logning, to-faktor login ved fjernadgang samt systemer sikret med autorisationer og adgangskoder.

En sådan konkretisering tjener flere formål. Det gør *for det første* den dataansvarlige i stand til at dokumentere, at vedkommende har handlet ansvarligt i sit valg af databehandler, og *for det andet* muliggør det et effektivt tilsyn, idet den dataansvarlige ved, hvad han skal kontrollere hos databehandlere, se mere herom netop nedenfor.

10.4.2. Indgåelse af en databehandleraftale

Når den dataansvarlige har sikret, at den valgte databehandler kan levere tilstrækkelig sikkerhed, skal parterne indgå en databehandleraftale, som opfylder de indholdsmæssige krav i forordningens artikel 28. Nedenfor ses en skematisk oversigt over disse krav:

Dokumenteret instruks
Genstanden for og varigheden af behandlingen
Behandlingens formål og karakter
Liste over typer af oplysninger og kategorier af registrerede
Dataansvarliges forpligtelser og rettigheder
Hvornår og under hvilke betingelser der må ske overførsel til 3. lande
Medarbejderautorisation
Sikring af, at personer hos databehandleren, som er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.
Sikkerhed
Sikring af, at databehandleren har forpligtet sig til at arbejde risikobaseret og på den baggrund implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger.

Databehandleren underretter den dataansvarlige efter at være blevet opmærksom på et brud på persondatasikkerheden.
Brug af underdatabehandlere
En bestemmelse der regulerer, hvornår og hvordan en databehandler må benytte underdatabehandlere. Bestemmelsen skal endvidere pålægge databehandleren fuldt ansvar for dennes brug af underdatabehandlere, samt at underdatabehandleren som minimum pålægges samme forpligtelser som databehandleren.
En bestemmelse der regulerer, hvornår Databehandleren skal underrette den Dataansvarlige om tilføjelser/erstatning af underdatabehandlere.
Pligt til at assistere den dataansvarlige
Så vidt muligt bistå databehandleren, ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder.
En forpligtelse til at bistå den dataansvarlige, hvor dette er relevant, med dennes overholdelse af: — Implementering af passende sikkerhedsforanstaltninger — Håndtering af databrud — Udarbejdelse af Konsekvensanalyser/DPIA
Sletning
En bestemmelse der pålægger databehandleren at tilbagelevere og/eller slette alle personoplysninger, som tilhører den dataansvarlige ved kontraktens ophør.
Dokumentation
Den dataansvarlige er ifølge lovgivningen forpligtet til at føre løbende og systematisk kontrol med databehandleren ud fra en risikobaseret tilgang. Databehandleraftalen skal derfor forpligte databehandleren til at stille alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i denne artikel, til rådighed for den dataansvarlige, herunder give mulighed for og bidrage til revisioner og inspektioner.

Det skal fremgå af aftalen, at databehandleren underretter den dataansvarlige, hvis den dataansvarlige anmoder om en kontrolforanstaltning, som ifølge databehandlerens vurdering vil krænke andre kunders/personers rettigheder.

Udover de formelle indholdsmæssige krav i forordningen er der en række forhold, som man bør overveje at tage stilling til i aftalen.

Mange databehandleraftaler indeholder et afsnit vedrørende ansvarsfordelingen mellem parterne. Her er der i udgangspunktet aftalefrihed, idet forordningen dog indeholder visse begrænsninger i artikel 82 og 83.

Dernæst er det oftest også relevant at regulere, hvad databehandleren kan kræve vederlag for. Databehandleraftalen pålægger databehandleren en række opgaver, der ligger ud over den egentlige databehandlerydelse, f.eks. at bistå den dataansvarlige med at sikre overholdelse af sine forpligtelser vedrørende passende sikkerhed. Dette sker dog "under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren", hvorfor bistandens omfang kan variere meget. Persondataforordningen regulerer ikke parternes mulighed for at kræve vederlag, hvorfor dette er et spørgsmål, der må aftales imellem parterne.

10.4.3. Særligt om løbende tilsyn med databehandleren

Der stilles også krav om, at den dataansvarlige løbende fører tilsyn med, at databehandleren overholder de forpligtelser, som denne er blevet pålagt i databehandleraftalen.

Forpligtelsen til at føre tilsyn fremgår ikke direkte af forordningen, men det er en forudsætning for, at den dataansvarlige kan påvise, at behandlingen af personoplysninger sker i overensstemmelse med reglerne og dermed kravet om ansvarlighed. Efter Datatilsynets opfattelse kan den dataansvarlige ikke leve op til sine forpligtelser, hvis en indgået databehandleraftale ikke følges op af et større eller mindre tilsyn.[10]

10. Datatilsynet 2018b, s. 2.

Et tilsyn kan ifølge Datatilsynets vejledning ske ved et fysisk besøg eller gennem skriftlig informationsindsamling.[11] Uanset formen vil tilsynet tage udgangspunkt i risikovurderingen og de sikkerhedsforanstaltninger, der i databehandleraftalen er aftalt imellem parterne.

Et *fysisk tilsyn* kan f.eks. omfatte undersøgelse af fysiske adgangsbegrænsninger, stikprøvekontrol af medarbejderes autorisation og håndteringen af fysiske dokumenter. Det *skriftlige tilsyn* kan bl.a. være baseret på relevante spørgsmål, organisationen selv stiller, en revisionserklæring og eventuelle opfølgende spørgsmål.

Hvad der vil være den mest hensigtsmæssige tilsynsform, vil afhænge af den konkrete databehandler, herunder en vurdering af, hvilke risici der er forbundet med den pågældende behandling af personoplysninger. Er der således tale om en databehandler, der behandler en stor mængde af oplysninger og/eller følsomme personoplysninger, vil der blive stillet større krav til omfang og hyppighed af den dataansvarliges tilsyn.

11. Ibid., s. 4.